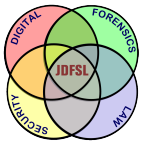
2017

Broadband router security: History, challenges and future implications

Patryk Szewczyk
Edith Cowan University, p.szewczyk@ecu.edu.au

Rose Macdonald
Edith Cowan University

Szewczyk, P., & Macdonald, R. (2017). Broadband Router Security: History, Challenges and Future Implications. *Journal of Digital Forensics, Security and Law*, *12*(4), 6. Available here.



THE JOURNAL OF
DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 4 Article 6

12-2017

Broadband Router Security: History, Challenges and Future Implications

Patryk Szewczyk
Edith Cowan University, Western Australia, p.szewczyk@ecu.edu.au

Rose Macdonald
rmacdon0@our.ecu.edu.au

BROADBAND ROUTER SECURITY: HISTORY, CHALLENGES AND FUTURE IMPLICATIONS

Patryk Szewczyk and Rose Macdonald
Edith Cowan University, Western Australia

ABSTRACT

Consumer grade broadband routers are integral to accessing the Internet and are primarily responsible for the reliable routing of data between networks. Despite the importance of broadband routers, security has never been at the forefront of their evolution. Consumers are often in possession of broadband routers that are rich in consumer-orientated features yet riddled with vulnerabilities that make the routers susceptible to exploitation. This amalgamation of theoretical research examines consumer grade broadband routers from the perspective of how they evolved, what makes them vulnerable, how they are targeted, and the challenges concerning the application of security. The research further explores the Australian roll out of a joint ISP; consumer extended public Wi-Fi network (Air), in which routers play crucial roles. The security of these networks is considered, and questions are explored, regarding consumer legal risks, particularly for consumers who opt-in to extend this service. This research paper concludes with recommendations for the development and introduction of Australian router security deployment standards.

1. INTRODUCTION

Australia is consistently identified as a major Internet user that will continue to be targeted by cybercrime. Some protection is afforded by specialised security software for computers. Asymmetric Digital Subscriber Line (ADSL) routers can complement specialised security software in counteracting the severity of cybercriminal activity. For the ADSL router to provide a layer of security, it requires adequate and an appropriate selection of security mechanisms and controls. The ADSL router typically operates in a discreet, reliable manner within Small office Home office (SoHo) environments - typically forgotten once the initial configuration phase passes. However, there is continual increase in research evidence depicting cyber-attacks specifically targeting or exploiting vulnerabilities within ADSL routers. Rumours further indicate that known vulnerabilities within ADSL routers may purposefully go unaddressed, allowing specific organisations remote access to a target network (Greenberg, 2017). The ongoing cyber-attacks demonstrate the need to protect an ADSL router correctly - using best practices and standards.

ADSL routers (also known as 'broadband routers,' but referred to hereafter as just 'routers') are essential in providing reliable network connectivity between computers, printers, tablets, the Internet of Things (IoT), and the Internet. The connections form networks, which may be small local networks, or larger external networks linking thousands of devices across vast areas. The required

network topology, scale, and purpose dictate the type or category of router hardware chosen to establish the connections. While enterprise grade routers provide the highest levels of functionality at a premium price, the vast majority of small business and residential premises do not require the premium functionality. The small business and residential market typically opt for SoHo routers, which provide consumers with the desired functionality and an intuitive Graphical User Interface (GUI) to simplify the configuration process.

Vendors continually incorporate advanced features and technologies into routers making them increasingly attractive to consumers. Common router features typically include a four-port Ethernet switch, high-speed wireless networking capabilities, network file sharing, printer servers, and scalability for integration with smart home technologies within a home network. These additional features whilst attractive to consumers may also create a range of supplementary vulnerabilities. The exploited vulnerabilities may have enabled cyber criminals to access a private network in an unauthorised manner.

Routers are the "work horses" of the SoHo Internet, controlling the flow of data between private and public networks. Unfortunately, there are ongoing security flaws embedded within routers, which may expose users and data to intrusions, through a range of attack vectors. Cyber criminals who recognise the opportunities and benefits in being able to control or remotely access routers for personal gain can exploit the security flaws within routers. For novice end-users, the router is often the only barrier segregating the user's data from the Internet. Many router vulnerabilities stem from poor firmware development and a lack of ongoing maintenance (Hampton & Szewczyk, 2015). In contrast, users also poorly configure routers during the initial configuration stage (Szewczyk, 2006). Inadequate security configuration may be attributed to end-users lacking accurate knowledge and an appropriate skillset to apply the ideal security settings. Despite end-users typically ridiculed for inadequately securing their routers, research has demonstrated that vendors are equally to blame with poor or inaccurate product literature to support and guide end-users through the configuration phase (Szewczyk, 2013).

2. HISTORY AND EVOLUTION OF NETWORK ROUTERS

The foundations of network routing were developed in the late 1960s by a closed academic group of researchers known as the Advanced Research Projects Agency (ARPA). The goal of the agency was to build a network of four Interface Message Processors (IMPs) to send data over phone lines. ARPA put out a tender for the development, which was won by a small company known as Bolt, Beranek and Newman (BBN) (Raytheon, 2011). In August 1968, the BBN group used "an off-the-shelf Honeywell 516 to design the I/O devices that would need to be added to the basic model to start writing the code that would reload crashed IMPs, pull packets into the machine, figure out how to route them, and send them on their way" (Raytheon, para.4, 2011).

On October 1st, 1969, the first set of characters were successfully transmitted over the new network and the Advanced Research Projects Agency Network (ARPANET) was founded. The IMP could support 50Kbps links between nodes (Duffy, 2009). The achievements of the group remained confined to those at ARPA, BBN and a small group of researchers until 1972, when a project titled, "The Technology of Packet Switching" was presented at the International Conference on

Computer Communication in Washington (Raytheon, 2011).

In 1980, Stanford University was the recipient of several Alto workstations and Ethernet networking boards from the Xerox Palo Alto Research Centre. Collectively, Stanford University staff and graduate students used this technology to develop what later became known as the 'Blue Box.' The Blue Box functioned as a multiprocessor, providing the capability for Stanford's schools and departments to communicate with each other. William Yeager, a research engineer at Stanford's medical school, had just completed writing a small routing program, which acted to connect computers in the medical department with those in the computer science department (Carey, 2001). Yeager's software program was a "multiprotocol network that linked Alto workstation, mainframes, mini-computers and printers" (Carey, 2001). Yeager went on to writing a more sophisticated program, which was able to route several protocols including the relatively new Internet Protocol (IP). Yeager's advanced software was designed for the twenty-four Stanford Blue Boxes that could be seen around the campus during that time (Carey, 2001).

In 1985, two Stanford staff members, Len Bosack and Sandy Lerner, who had been involved in the Blue Box project, allegedly asked Yeager for his software code so they could modify it to route only Internet Protocols. Controversially, in the previous year, Bosack and Lerner had founded a company called Cisco, and used Yeager's work to propel the development of Cisco products. This became the subject of legal debate in future years (Carey, 2001). Bosack and Lerner would later return the capacity for Yeager's code to route protocols other than just IP, enhancing the functionality of the products they developed. Through 1986, Cisco introduced its first commercial multiprotocol router, called the Advanced Gateway Server (AGS) into the communications market, which supported the Transmission Control Protocol (TCP), Internet Protocol (IP) TCP/IP (Duffy, 2009).

IP router architecture has continued to evolve in step with the complex and sophisticated networks of the protocols they support. Today, a SoHo router may "fully utilize the capabilities of specialized hardware and integrates an endless suite of functionalities, ranging from raw packet forwarding through traffic shaping, packet queuing, access control, Network Address Translation (NAT) with connection tracking all the way to distributed network protocols" (Csaszar, Enyedi, Hidell, Retvari, & Sjodin, 2012). There was one critical oversight made by engineers, developers and researchers who actualised the future of our communications. The oversight was security, and through its absence, forged a mindset of functionality over secure communications that persists today.

3. ROUTERS AS AN ATTACK PLATFORM

The SoHo router is an ideal target for cyber criminals. Consumers obtain a router through their Internet Service Provider (ISP) or purchased online or via a computer retail outlet. In either instance, the router typically encompasses minimal or no security by default. The lack of security reduces the cumbersome task of progressing through the configuration phase for the novice end-user. However, minimal security on the router also simplifies the attack process for cyber criminals. A successful attack on the router may reward the cyber criminal with direct access to the router's operating system (firmware), to the prized internal network consisting of all the connected devices, and to the data stored and traversing the network. As the inclusion of IoT and smart devices continues to further increase

in quantity within home environments, there are additional incentives for cyber criminals who exploit the router and network. From such a privileged position, the intruder can control the network whilst accessing and misusing the data stolen from it. The consequences for the victim may include loss of personal information, financial data, account passwords, and their identity.

Vulnerabilities associated with coding flaws in the firmware development stage is an ongoing issue. Yang (2016) highlighted this issue in a DEFCON presentation in 2015. Yang, (2016) discovered a number of zero day vulnerabilities in his work as a security researcher and ethical hacker on a range of SoHo centric routers. Vulnerabilities included vendor backdoors, debug interfaces left active, concerns with the ease at which intruders could gain access to shells, arbitrary file reads, stack overflows and unauthorised remote access via services such as Universal Plug and Play (UPnP) (Yang, 2016). Security researcher Pierre Kim publicly disclosed a large quantity of zero day vulnerabilities for D-Link routers in 2017, following numerous failed communication attempt to inform D-Link of the security issues (Osborne, 2017; Kim, 2017). The reluctance by vendors to listen to security researchers and the community who discover vulnerabilities further demonstrates the issues with progressively addressing known security vulnerabilities within routers.

Irrespective of ethics, all system penetrations begin with reconnaissance, and search engines such as Shodan.io provide a perfect opportunity for attackers to identify vulnerable targets and gather intelligence. Shodan.io purports to be the "world's first search engine for Internet connected devices," (Shodan.io, 2016) otherwise known as the Internet of Things (IoT). Users can access all the features of the search engine, which can pull information from thousands of different sources. Shodan.io is proving to be a powerful tool for identifying vulnerable clients, and to demonstrate its capacity a number of search queries targeting SoHo connections to micro_httpd servers were conducted in this research. The results were troublesome with 615,000 SoHo routers identified with open ports in response to one search query (port:80 micro_httpd). Similar searches were run on other popular servers such as Apache (port:80 Appache httpd) which returned more than 2,000 vulnerable router hits. Valuable information is presented to the user in the search results, including the business or company name of the target, location, IP address, name and model of the router, and the ports and services that are open. A convenient link is also provided directing the user to the router's web interface page where default usernames and passwords can be tested. If successful, the attacker may proceed with a range of attacks as depicted in the following section, thus compromising multiple hosts.

4. ATTACKS ON SOHO ROUTERS

4.1 Cross-Site Request Forgery

The aim of a Cross-Site Request Forgery (CSRF) attack is to direct the user to a web page controlled by the attacker where malicious code is embedded in web pages. The code acts to transfer sensitive data to the attacker without the knowledge of the end-user. Account details, passwords, financial information, and other sensitive information is stolen in this process. Routers are vulnerable to CSRF attacks because they are usually configured with through a web browser connected to an embedded web server within the router. On successful completion of such an attack, the router's Domain Name System (DNS) entries may be altered or device settings altered to make the targeted network

additionally susceptible to attacks (Router Check, 2016). Land (2017) discovered that 54% of examined routers contained a CSRF specific vulnerability. Despite many routers encompassing a CSRF vulnerability (Rotenberg et al., 2017), D-Link routers are at the forefront of largest quantity of devices encompassing the issue (CVE-2015-5999, 2015; CVE-2017-5633, 2017; CVE-2017-6411, 2017; CVE-2017-7398, 2017) with exploits focusing on altering the configuration, or diminishing the overall state of security.

4.2 Information Disclosure

Information Disclosure attacks are categorised by attempts to acquire specific system information through the CPE (Customer Premises Equipment) WAN (Wide Area Network) Management Protocol (CWMP). Technical support personnel within ISP departments leverage CWMP to remotely trouble shoot or administer changes to routers. In 2015, several Netgear SoHo routers were identified as having an information disclosure issue that allowed attackers to access unauthorised information (Constantin, 2014). The vulnerability exploited the Simple Object Access Protocol (SOAP) by "sending HTTP requests with a blank form and a 'SOAPAction' header" (Constantin, 2014). Administrator information including the model, serial number, and firmware version of the router targeted which was available to intruders (Constantin, 2014). The CWMP service facilitated a variant of the Mirai malware specifically exploiting SoHo routers and modems (Antonakakis et al., 2017). The extent of the damage caused by the Mirai malware targeting German focused routers exceeded 900,000 (Kolias, Kambourakis, Stavrou & Voas, 2017).

A directory traversal vulnerability leaves users open to intruders attacking SoHo routers remotely. A flaw in the firmware allows attackers to access restricted directories, such as the router's configuration settings, administrator password hashes, ISP usernames and passwords, Wi-Fi passwords and client or server authentication credentials (Armasu, 2015). In 2015, one directory traversal vulnerability appearing in the *webproc.cgi* component of the target router allowed an attacker to extract a *config.xml* file containing authentication credentials. In this particular case, more than 700,000 vulnerable routers involving multiple vendors were identified. It was later discovered that each vendor had used firmware developed by the same third-party company (Armasu, 2015).

4.3 Cross Site Scripting

There are three main cross-site scripting attacks, known as 'Document Object Model' (DOM), 'Persistent,' and 'Non-persistent attacks.' In each of the attacks, the intruder injects malicious JavaScript or HTML code into the web application of the router. This provides the attacker with elevated privileges from which modifications to the firmware settings result in a network hijack. The attacker needs to be authenticated by the router to carry out this attack (Independent Security Evaluators & Holcomb, 2013). However, once authenticated targeted data includes the username and password set up page of Network Attached Storage (NAS), the device name of the USB_advanced.htm or the network key to the wireless setup page (NIST, 2014).

4.4 Authentication Bypass

SoHo routers require user authentication to access the router's web interface where a variety of configuration and function modifications occur. Any flaw in the authentication method that allows an intruder to gain unauthorised access is considered an authentication attack. The most basic of these attacks involves the use of default username

and passwords, which are easily discoverable. A number of public websites provide lists of vendors' default username and password details. If the owner or administrator of the targeted router has failed to change the default authentication credentials, then access to the router's configuration pages is simplified. An alternate and common authentication bypass attack is through Structured Query Language (SQL) injection technique. An SQL injection attack operates by running malicious or altered SQL queries against a database or web server. A successful SQL injection attack may result in unwanted information disclosure, compromised data integrity, compromised data availability and remote command execution (CISCO, 2016). Cutlip (2012) examined the Netgear WNDR3700 series broadband wireless routers, documenting the presence of a vulnerability within the miniDLNA server making the router susceptible to SQL injection, yielding remote root-level access. Alternate vendors are not immune to the vulnerability with D-Link encompassing numerous Authentication Bypass issues through an SQL-Injection vulnerability as per CVE-2013-5945 (CVE-2013-5945, 2013; EDB-ID: 30062, 2013).

UPnP vulnerabilities (SSDP discovery and SOAP) to the Internet side of the device Universal Plug and Play (UPnP) is a protocol standard that allows communications between computers and network-enabled devices. The protocol is enabled by default on millions of systems, including routers where authentication is rarely implemented. The literature suggests this feature is one of the most exploitable services available to an attacker. The issues stem from poor development and implementation of the protocol, with much of the literature pointing to a vast number of systemic security issues. UPnP enabled routers allow devices and applications on the network supporting it to configure themselves and perform port forwarding functions without authentication (Router, 2016).

4.5 Unencrypted Password Storage

In 2013, research conducted by RAPID7 identified forty to fifty million networked enabled devices that were vulnerable to exploits using the UPnP protocol. Nearly all the vulnerable devices identified were SoHo routers. Critically, "sixty percent of routers tested allowed users to login to their administrative console using passwords sent wirelessly via HTTP – clear text broadcasts over the air: Only 40 percent of the routers tested provided HTTPS connections and only 20 percent used it by default" (Fogarty, 2014). This is an unacceptable risk. End-users are exposed to Man in the Middle attacks (MITM) where network traffic is intercepted and directed to the attacker who is primed to capture these details and use them to further compromise systems. According to Fogarty, (2014) the danger is critical if unsecured wireless services are used, such as those found in public places, small businesses and closely packed living environments (Fogarty, 2014). This is due to signal leak whereby the presence of wireless access signals are detectable beyond the boundaries of where it is required.

4.6 Unauthenticated Hardware Linking

According to Holcomb (2013), the Netgear WNDR7400 router was found to be vulnerable to an attack which is carried out by sending HTTP requests to the router's web management application. The process causes the routers internal and external storage to link to an attacker controlled Ready Shared Cloud Account, which facilitates access to files hosted by Ready Shared enabled routers. Ready Share Cloud is a feature provided by Netgear that allows the consumer to access remotely a USB storage device that is

connected to a USB port on the router (Netgear, 2011). A successful attack will provide the intruder with access to all files stored on the external storage of the SoHo router (Independent Security Evaluators & Holcomb, 2013).

Remote attackers may modify firewall rules or access private media files using Digital Living Network Alliance (DLNA) DLNA is an industry wide standard that allows data to be shared over a home network. It includes organisations and vendors who comply with the standard to allow music, movies and other data shared across televisions, smartphones, computers and other devices. Many routers are able to link DLNA compliant products across home networks with the exception of Apple TV, which is currently not supported (Laughlin, n.d.). DLNA uses UPnP for media management, discovery and device control which simplifies the set up and use of device streaming across the home network (Charan, 2012). The more devices connected to the network the greater the opportunities for attackers to target UPnP vulnerabilities.

4.7 Buffer Overflows

Buffer overflows are a critical security vulnerability that occurs because of programming errors affecting memory. These can occur in any operating system. The consequence of a buffer overflow is that attackers can inject malicious code into the buffer and if the code executes; the attacker can take control of the system. A recent buffer overflow vulnerability was identified in several D-Link router models, reported to the National Institute of Standards and Technology (NIST) on 25 August 2016. In this case a "stack-based buffer overflow in dws/api/Login allowed remote attackers to execute arbitrary code via a long session cookie" (CVE-2016-5681, 2016).

4.8 Remote Administration Enabled

Remote administration allows the user and anyone else with credentials to access the administration page of the user's router over the Internet from an external location. In order to remotely access a router, the IP address, port number and administrative username and password is entered into a web interface. Users should disable this feature unless there is a genuine need to access the router remotely. This is because enabling remote access is akin to running an open port, which is an attractive target to an attacker.

According to Constantin (2014), many ISPs are deploying SoHo routers to their customers with remote access enabled, allowing the vendor to remotely manage and update devices. CWMP is used to troubleshoot technical problems remotely (Constantin, 2014). It is estimated that in 2011, 147 million devices had the CWMP protocol enabled, of which seventy percent were SoHo routers. The remote management protocol typically operates on port 7547 and is the second most commonly encountered service port after port 80 (Constantin, 2014).

5. CHALLENGES IN SECURING SOHO ROUTERS

The myriad of vulnerabilities identified in the preceding section provides insight into the challenges facing governments, cyber security professionals, vendors, businesses and consumers in securing SoHo routers. Yang (2016) suggests that the practice of customising open source software to suit a specific router in combination with programmers lacking sufficient knowledge of programming languages is a significant issue in developing reliable, bug-free code. Yang's view is supported through the reverse engineering of firmware, which demonstrated that some routers were encompassing security vulnerabilities exceeding ten years in age

(Hampton & Szewczyk, 2015). Yang (2016) describes the practice of poor firmware development as leading to the production of a range of coding flaws, which are primed for exploitation. Fogarty (2014) argues that wireless routers are riddled with security holes stemming from design goals that focus usability over security. Given that vendors are often praised with being first to the market with innovation, it is not surprising that security is an aspect that is typically overlooked.

Routers purchased in-store typically have security features disabled by default and backdoors left open. Consumers purchasing ADSL SoHo routers in-store cannot assume the device was shipped with security pre-configured. Furthermore, unlike a traditional operating system, the end-user is not prompted to update the device during the initial configuration process. The literature highlights a persistent mindset of functionality over security. According to Sericon Technology (2015), router software issues extend to vendors, failing to fix problems when identified coupled with users failing to upgrade firmware even when a fix may have been made available for a considerable timeframe. The disconnect between vendors and end-users creates a risk focused environment with routers encompassing little security and well documented vulnerabilities circulating in the 'hacking' community.

According to Horowitz (2016), numerous issues exist when attempting to update router firmware. These include but not limited to: updates modifying router settings that the consumer is unaware of, complicated processes with poor documentation, methods to update firmware varying and too often requiring manual effort, firmware update processes 'bricking' or making the router non-functional, and a lack of notification of the availability and importance of an update for consumers. Poor firmware update processes are further extenuated through vendors using 'features' as a driver to promote firmware updates rather than security issues being addresses. Unless an end-user understands a benefit in an advanced feature set, the likelihood of the update being applied is diminished.

Programmers may create undocumented backdoors during the firmware development phase, so they can interact with products during the development phase. The programmer may wish to save data and test and/or modify the program when things go wrong (Haag, Cummings, & Rea 2016). Programmers may opt to close backdoors before the device is released to the public but may also forget to do so, or purposely leave one or two open, so they can access the program post sale. This practice exposes all routers supporting the firmware to attack and consequently all the clients associated with it (Haag et al., 2016).

The United States Computer Emergency Readiness Team (US-CERT), the Independent Security Evaluators (ISE), and several security professionals all highlight concerns about ISPs deploying pre-configured routers. The consensus appears to be that too often, routers are deployed with limited security, and consumers do not have the knowledge, interest, or willingness to dedicate the time required to alter pre-configured settings (US-CERT, 2011). Researchers in Spain (Folgado, Rodríguez, & Sanz de Castro, 2017) examined twenty-two models of SoHo routers from different vendors, most of which were deployed by ISPs. The researchers found sixty flaws across the twenty-two models tested. This further supports concerns that ISPs do not support end-users in pursuing a cyber security conscious mindset.

Vendors and ISPs provide limited information to consumers to assist them in securing SoHo routers. Szewczyk & Valli

(2009) described the absence of consumer support and poorly written documentation as a significant risk. They were particularly critical of the quality of vendors' user manuals, citing a lack of detail, inadequate instruction, the use continual use of unexplained jargon and a lack of consistency in content as being major barriers to consumers having neither the confidence nor encouragement to implement adequate security. Szewczyk & Valli (2009) conducted an examination of vendor documentation over a four-year period and concluded not a single vendor manual could be described as 'ideal' or adequately support a novice end-user in applying ideal security practices to their router. "Attempting to configure and secure an ADSL router is not designed to be a trivial task for the average end-user" (Szewczyk & Valli, 2009). This statement raises the question about who should be responsible for provisioning adequate security. End-users need protection, but also require the set-up of networks to be sufficiently simple to allow them to participate in and understand the set-up process. However, if a router is secured by default, and thus potentially cumbersome to implement in a home network – would this process potentially encourage end-users to purchase an alternate product with less security but improved usability.

According to Independent Security Evaluators (ISE), (2015), SoHo routers are continually vulnerable due to the manner in which they are deployed and used in locations such as; coffee shops, libraries, small businesses and high density living communities where signals can bleed through walls and someone could 'listen in'. The ISE report concluded that compromised routers could be used to perform a man in the middle attack and thus enabling a more sophisticated attack to be performed on devices connected to the router. Specific threats may include but are not limited to network sniffing, traffic rerouting, DNS poisoning, denial-of-service attacks, or impersonating servers (Independent Security Evaluators, 2015).

6. ISP EMERGING ROUTER DEPLOYMENT

Throughout many countries around the world, ISPs have committed to creating large scale ISP influenced consumer provisioned public Wi-Fi networks. Companies such as Fon in Europe, Comcast in America, and Telstra in Australia are examples of companies that have established this shift in our public network environments. Each scheme works through the co-operation between the ISP and their consumers. ISPs deploy routers to their consumers that are pre-configured to allow the consumer to 'trade-off' a portion of their home Internet bandwidth to make it publicly available for others to use.

Essentially, the ISP provides the connection to the Internet and the consumer extends the ISP's network by turning their SoHo network into a Wi-Fi hotspot. The benefit to the participating consumer is that their 'trade-off' is effectively offset by their ability to use 'hotspots' provided by other consumers who have similarly opted into the program. The commonality amongst users is they share the same ISP provider and in Australia, opt-in to the service (Telstra Corporation Limited [AU], 2016). As part of their launch, Telstra extended its Telstra Air free service period to customers until 27 March 2017, and currently boasts 650 thousand hotspots across Australia (Telstra Corporation Limited [AU], 2016b). According to Kidman (2014), Telstra anticipates creating approximately 2 million hotspots nationwide. Additional benefits for Telstra customers include free access to 19 million hotspots internationally, through Telstra's partnership

with European Company, Fon (Telstra Corporation Limited [AU], 2016b).

The routers deployed by Telstra for the 'Air' network are named Telstra Gateway and Gateway Max. Each device supports Hybrid Fibre Coaxial (HFC), ADSL, VDSL and NBN and cost $168.00 AUD for the 'Telstra Gateway' and $264.00 AUD for the 'Gateway Max.' Consumers can purchase the Air compatible routers outright or pay through a subscription agreement. Alternatively, consumers can purchase a day pass for occasional use. The service requires use of the Telstra Air application, which is compatible with iOS and Android devices. The customer must log in to the application using a username and password, which ensures all data used is deducted from the guest user's private broadband account. The application will search for and automatically connect the customer's mobile computing device to the nearest hotspot when detected, thereby providing customers with an extended public Wi-Fi service (Telstra Corporation Limited (AU), 2016a).

Technical security information about the Telstra Air network and associated hardware is presently scarce. The Air network does make use of two SSIDs, one for the public network and one for the private network and can operate on either the 2.4 GHz or 5 GHz frequencies. A scan of the local area during this research identified two public prefixes, namely Fon Wi-Fi and Telstra-Air. Telstra allows customers to change the network names, as long as the public side of the network encompasses a prefix identifying it as an Air service.

Instructions on setting up the Telstra ADSL gateway is presented on the Telstra website step-by-step with graphical images to assist customer comprehension. However, no information is provided with respect to the configuration of default security settings. Telstra does state that "your Wi-Fi name and password can be found on the fridge magnet you received with your gateway" (Telstra Corporation Limited [AU], 2016b). This is an obvious security concern and it is recommended that ISPs avoid providing the names and corresponding security keys of customer networks on products that consumers are likely to keep within 'public' areas of their homes. Fortunately, Telstra does provide information on how customers can change these details and manage other ADSL settings through the management console. Telstra also appears committed to ensuring firmware updates on all devices to remain current, maintaining a policy of updating firmware automatically through their remote management system. The security trade-off of remote management is perhaps a considered risk adopted by them and it is hoped that mitigation strategies against remote management attacks have been implemented.

Security and other advice is offered to Telstra customers through their crowd support and the knowledge base community services. Telstra (2016) is cautious enough to inform customers to be careful with Telstra Air communications, advising communications between the Wireless Access Point (WAP) (ADSL router) and device remains unencrypted and therefore the service is not recommended for sensitive communications such as banking.

"Most public Wi-Fi networks, including Telstra Air, are unencrypted or open and potentially unsafe. When you're connecting to an open network, check for the padlock icon in the address bar of your device's web browser. This represents another layer of security. We recommend not using Telstra Air, or any public Wi-Fi network, for things like Internet banking or sending and receiving sensitive materials. Information for families Public Wi-Fi, including Telstra Air, is available in many

places across Australia and is easy to access" (Telstra Corporation Limited [AU], 2016.)

According to Kidman (2014), Telstra has always intended to deploy 'normal Wi-Fi' security on the public side of the network and if Telstra's partner Fon, can be used as a template to explore security features of Telstra Air products, it may be inferred that the default encryption standard is Wi-Fi Protected Access 2 (WPA2). Wired Equivalent Privacy (WEP), WPA and a no encryption option, often called 'open' are also supported. Fon devices support three encryption protocols namely, Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and TKIP/AES (mixed mode) (Gustafsson & Thor, 2007). Further research is required if default and optional setting configurations provided by Telstra are to be fully understood and in the best interest of consumers.

In America, Comcast provides the same or similar expanded Wi-Fi service through its 'XFINITY' hotspot feature. Like Fon and Telstra Air, Comcast describes their service to consumers as an extended Wi-Fi network, "Your XFINITY Wireless Gateway broadcasts an additional "xfinitywifi" network signal for use with XFINITY WiFi. This creates an extension of the XFINITY WiFi network right in your home that any XFINITY Internet subscriber can use to sign in and connect. This XFINITY WiFi service is completely separate from your secure WiFi home network" (Hoffman, 2014a).

Proponents of this consumer extended Wi-Fi network argue that consumers are provided with greater safeguards when compared to open public Wi-Fi networks because users must register and opt-in to use the service, with all Internet activity linked to the guest's private user account. Critics point to the ease in which false accounts or rogue hotspots can be created, along with fake sign-in pages, effectively creating a vacuum from which all sorts of sensitive data can be stolen. Consumer-oriented man-in-the-middle devices such as "Wi-Fi Pineapples" are exemplars of devices that could be used to impersonate and intercept traffic within these networks (Acuna et al., 2017).

In considering these arguments, it is proposed that opt-in services such as Telstra Air, Fon, and Xfinity provide no greater levels of security to users of public Wi-Fi services when compared to traditional open Wi-Fi hotspots. Network traffic on 'Air' remains unencrypted and no mitigation strategies are proposed to protect users from accessing rogue access points. For the provider of the extended service, little risk is apparent, as guest users sit on the outer side of a separate network and all guest activity is logged and associated back to the guest's private broadband account. For the consumer provider's private network, there appears to be no change to the vulnerability status beyond that which exists as a regular end-user of Internet services. The private network remains as secure as the configuration of their SoHo router is.

7. CONSUMER LEGAL RISKS

The legal issues regarding the Internet and Internet-related services are complex and the following presentation of material is designed to promote discussions about these issues. Consumer liability hereafter is defined as the burden of responsibility imposed on an adult person to secure a Wi-Fi router owned or operated by him or her. The test will be whether a burden exists or may exist in Australia in future years. Watkins (2013) argues that although criminal liability for the malicious actions of a third party accessing an unsecure wireless network remain largely ambiguous, cases have emerged whereby unlikely individuals are being held accountable

for the "negligent operation of a wireless network." The pre-eminent case regarding consumer liability and the provision of public Wi-Fi networks took place in Germany in 2010. The case, 'Tobias Mc Fadden v Sony Music Entertainment Germany GmbH' (2010) has been well documented in several media publications and law journals in Europe and elsewhere. The case centred on a small music store business that provided free Wi-Fi access to its customers, some of whom used the service to illegally download songs owned by Sony Music Entertainment (Grieshaber, 2010). 'Sony' sought to sue Tobias McFadden, the owner of the store, for indirectly breaching copyright laws; by failing to prevent the use of his public Wi-Fi service for illegal downloading. The German court made three significant rulings in this case,

1. "Internet users need to secure their private wireless connections by password to prevent unauthorized people from using their web access to illegally download data" (Grieshaber, 2010).
2. "Internet users can be fined up to euro 100 if a third party takes advantage of their unprotected WLAN connection to illegally download music or other files, the Karlsruhe-based court said in its verdict" (Grieshaber, 2010).
3. The court did not find the provider of the service, Tobias McFadden liable for the criminal conduct, namely the downloading of songs (Grieshaber, 2010).

In Australia at present, individuals and businesses are not required by law to secure SoHo routers, whether for private or extended for public use, and therefore are not currently legally liable for activity conducted by a third party using it. However, to date, Australia has not been challenged in the same way as seen in the 'McFadden,' 'Sony' case, where breaches of copyright occurred through individuals accessing a third-party Wi-Fi service. More recently, and despite the German court ruling that passwords were required to secure private networks, the German Government has proposed new legislation designed to reduce the burden of responsibility on business owners and individuals providing public Wi-Fi networks. The proposed legislation is to reflect the German Government's position that individuals and businesses are not liable for illegal activity arising from Internet activity they provide, as long as the service is only made available to users, "who have declared not to commit any rights violations in the context of the use" (Out-Law.com, 2016). The Australian Government may need begin considering a similar approach in order to protect Australian citizens who might be unknowingly but similarly exposed to litigation by large corporations imposing their copyright protections. It is unclear whether the absence of a requirement to secure Wi-Fi services is sufficient to ward off these litigation attempts.

Placing the onus of responsibility on consumers alone to adequately secure their SoHo router is unreasonable, especially in the absence of adequate instruction, adequate set-up and configuration documentation, or any legal requirement for developers, vendors or ISPs to meet minimal security standards. If a minimum standard of security is the desired outcome, then the onus of responsibility should be on developers, vendors, and ISP providers who possess both the technical knowledge and expertise to deploy devices that could comply with set minimum-security standards. In support of this assertion, a recent settlement between ASUSTeK (ASUS) and the U.S. Federal Trade Commission (FTC) is reviewed.

On 23 February 2016, the U.S. Federal Trade Commission (FTC) entered into a settlement with ASUSTeK (ASUS) after it was alleged that ASUS had failed to use

'reasonable security' to protect consumers' personal information that was exposed in a security breach in February 2014. A total of 12,900 consumers' storage devices containing personal data were exposed in the breach (Charfoos, Feld, & Kadish, 2016). ASUS had previously claimed that their routers "protect consumers from any unauthorized access, hacking, and virus attacks" and "protect [the] local network against attacks from hackers" (Charfoos et al., 2016). Upon review, the routers were shown to have several vulnerabilities in the firmware due to design flaws and were inadequately secured. Allegations that ASUS had also failed to notify customers about how to mitigate the risks once identified also formed part of the original complaint (Charfoos et al., 2016). The terms of the settlement are comprehensive, with the main outcomes including a requirement for ASUS to introduce a comprehensive security plan to ensure routers produced by them "protects the privacy, security, confidentiality, and integrity of information transmitted through the routers" (Charfoos et al., 2016). In addition, ASUS will be subjected to audits for the next 20 years (Charfoos et al., 2016).

8. FUTURE RECOMMENDATIONS

Several recommendations are made in accordance with the outcomes of this research. A discussion is encouraged between policy makers, ISPs, and vendors about the introduction of legislation that places a burden of responsibility on vendors, developers and ISP providers to meet minimum-security standards when selling or deploying SoHo routers in Australia. It is suggested that at a minimum standard should include:

- Security to be at the forefront of all firmware development, with increased testing and transparency of all firmware placed into the public domain.
- SoHo routers not to be deployed or sold with default administrative usernames and passwords. This could theoretically minimise the exploitation of devices, which are accessed using simplistic brute-force approaches encompassing common usernames and passwords.
- Removing weak or obsolete Wi-Fi security protocols that are known to be easily exploitable and incorporating WPA2/AES security protocols as standard.
- SoHo routers to be deployed or sold with remote administration disabled or if enabled, clearly documented that it is enabled (i.e. informing the end-user), specifying why it is enabled, the benefits and risks towards the consumer of it being enabled and how it can be disabled.
- Improved methods for providing and applying firmware updates, and consistent standards for vulnerability disclosures and notifications to be developed.
- Minimum standards for content in user manuals to be established. The standard should clearly document what information must be included in the user manual, and standardised terminology that is easily understood by the end-user agreed upon by ISPs and vendors.
- A significant increase in consumer education and training programs regarding SoHo router security, risks and mitigation strategies, and cyber security in general.

SoHo router security is influenced through both technological and human factor challenges. For a lengthy period, end-users have had the opportunity to control and influence the state of security implemented and used on routers. However, preceding research

suggests that end-users do not always apply optimum security practices on their router. Furthermore, vendors do not necessarily deploy updates or address security vulnerabilities within a timely manner. Subsequently, the aforementioned recommendations enable routers to make use of baseline security standards thus minimising common and simple threats from targeting routers, for instance bandwidth theft resulting from open or WEP based wireless networks. End-users can be continually encouraged and influenced to make security conscious decision, but history has demonstrated that convenience will always be at the forefront of how consumers utilise technology. Convenience, coupled with end-users lacking an understanding, will persistently result in non-ideal practices being employed on routers. By creating a secure standardised baseline, end-users are not given the opportunity to diminish the state of security and thus forced to conform to a minimal level of implemented security.

9. CONCLUSION

It is evident that SoHo routers were not designed by vendors with security at the forefront of their development. In contrast routers have undergone a rapid expansion of add on features, with usability and functionality prioritised over security. The consequences of this approach are easily recognised with numerous vulnerabilities embedded in the firmware exposing hundreds of thousands, if not millions of consumers around the world to attacks on a continual basis. Search engines such as Shodan.io have capitalised on publicly exposed weaknesses of IoT devices. Strategic searches are easily used to obtain detailed information about devices, which may serve in assisting attackers to identify and select vulnerable targets. As large corporations move even further into creating worlds conditioned by our online behaviours, collecting information about what consumers do, where they go and why they do it, even more of our lives will be exposed. ISPs are expanding the geography of our connections. Consumers are opting into ISP provisioned services that engulf them in a web of public hotspots they help to create. In Australia, there is currently minimal publicly accessible information on the security features enabled upon deployment of ADSL routers used by consumers to contribute to this expanded Wi-Fi service. On the surface, it appears there are advantages for the consumer knowing that all guest connections are logged against the guests' private account; however, no information or discussion is available that either describes or discusses mitigation strategies to offset the risk of users joining rogue hotspots.

To mitigate the ongoing and prevalent issues identified in this paper, both technological and human factors must be altered to accommodate the novice end-users – who make up a significant proportion of end-users in Australia. From a technological perspective, security must be enforced, rather than be optional. Router vendors are at the fundamental level to support good security practices. For instance, the option for an end-user to utilise the default authentication credentials, during the initial configuration process of the device, should not be restricted. The selection of adequate passwords should be enforced and enhanced through password meters to demonstrate visually the soundness of a password by today's standards.

Consumers must begin to understand the risks involved in online environments and take a legitimate interest in their security. While it is unreasonable to transfer any technical burden for securing devices, which are inherently insecure onto consumers, they must recognise the burden of risk they carry. Consumers and policy makers must demand

responsible action; they must insist that security is at the forefront of all firmware development. Governments and policy makers must begin to enforce minimum-security standards. These should outline the minimum-security features that are to be enabled on upon the deployment of all ADSL SoHo routers to the general population. Unfortunately, too many consumers are at risk because the window to their networks (and their lives) is wide open, and sadly, many consumers are misinformed with how easily accessible they truly are.

REFERENCES

Acuna, V., Kumbhar, A., Vattapparamban, E., Rajabli, F., Guvenc, I. (2017). *Localization of WiFi Devices Using Probe Requests Captured at Unmanned Aerial Vehicles.* Paper presented at the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA

Antonakakis, M., April, T., Bailey, M., Bursztein, E., Cochran, J., Durumeric, Z., . . . Sullivan, N. (2017). Understanding the Mirai Botnet. Paper presented at the 26th USENIX Security Symposium, Vancouver, BC, Canada.

Armasu, L. (2015, March 20). 'Directory Traversal' Flaw Exposes Over 700,000 Routers to Remote Hacking. Retrieved 9 October 2016, from http://www.tomshardware.com/news/directory- traversal-flaw-router-hacking,28795.html

Carey, P. (2001, January 12). A start-up's true tale (12/01/2001). Retrieved 8 October 2016, from http://pdp10.nocrew.org/docs/cisco.html

Charan, S. (2012, November 7). HACK TRACK: DLNA (DIGITAL LIVING NETWORK ALLIANCE): Retrieved from http://hacktrack-2012.blogspot.com.au/2012/11/dlna-digital-living-network-alliance.html

Charfoos, D. G. P.-A. D., Feld, J. S., & Kadish, J. K. (2016, March). ASUS Settlement: FTC Continues to Focus on Privacy and Data Security Enforcement | Lexology. Retrieved 16 October 2016, from http://www.lexology.com/library/detail.aspx?g=882dd152-54e2-4bd3-9c83-1f042aa60005

CISCO. (2016, February 15). Understanding SQL Injection. Retrieved 9 October 2016, from http://www.cisco.com/c/en/us/about/security-center/sql-injection.html

Constantin, L. (2014). Many home routers supplied by ISPs can be compromised en masse, researchers say. Retrieved 23 October 2016, from http://www.pcworld.idg.com.au/article/552058/many_home_routers_supplied_by_isps_can_compromised_en_masse_researchers_say/

Csaszar, A., Enyedi, G., Hidell, M., Retvari, G., & Sjodin, P. (2012). evolution_of_router_architectures_and_ip_networks.pdf. Retrieved 11 August 2016, from https://www.ericsson.com/res/thecompany/docs/journal_conference_papers/packet_technologies/evolution_of_router_architectures_and_ip_networks.pdf

Cutlip, Z. (2012). SQL Injection to MIPS Overflows. Retrieved from https://media.blackhat.com/bh-us-12/Briefings/Cutlip/BH_US_12_Cutlip_SQL_Exploitation_WP.pdf

CVE-2013-5945. (2013). CVE-2013-5945 Retrieved from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5945

CVE-2015-5999. (2015). CVE-2015-5999 Retrieved from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5999

CVE-2016-5681. (2016). CVE-2016-5681 Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5681

CVE-2017-5633. (2017). CVE-2017-5633 Retrieved from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5633

CVE-2017-6411. (2017). CVE-2017-6411 Retrieved from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6411

CVE-2017-7398. (2017). CVE-2017-7398 Retrieved from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7398

Duffy, J. (2009, February 9). Evolution of the router. Retrieved 11 August 2016, from http://www.networkworld.com/article/2870329/lan-wan/evolution-of-the-router.html

EDB-ID: 30062. (2013). D-Link DSR Router Series - Remote Command Execution. Retrieved from https://www.exploit-db.com/exploits/30062/

Fogarty, K. (2014, February 18). Home Routers Pose Biggest Consumer Cyberthreat. Retrieved 1 October 2016, from http://insights.dice.com/2014/02/18/home-routers-pose-biggest- consumer-cyberthreat/

Folgado Rueda, Á., Rodríguez García, J. A., & Sanz de Castro, I. (2017). Revisiting SOHO Router Attacks. *Magdeburger Journal zur Sicherheitsforschung*, 14, 797–814. Retrieved August 10, 2017, from http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_054_Rueda_SOHORouter.pdf

Greenberg, A. (2017). Wikileaks Reveals How the CIA Could Hack Your Router. Retrieved June 15, 2017, from https://www.wired.com/story/wikileaks-cia-router-hack

Grieshaber, K. (2010, May 12). German court orders wireless passwords for all. Retrieved 22 August 2016, from http://www.nbcnews.com/id/37107291/ns/technology_and_science-security/t/german-court-orders-wireless-passwords-all/

Gustafsson, J., & Thor, D. (2007). Security Risk Evaluation of the FON Network. IEEE, Sweden. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4389894

Haag, S., Cummings, M., & Rea, Jn, A. (2016). Backdoors. Retrieved 15 October 2016, from http://highered.mheducation.com/sites/0072834110/student_view0/chapter13/backdoors.html

Hampton, N., & Szewczyk, P. (2015). A survey and method for analysing SoHo router firmware currency. Paper presented at the 13Th Australian Information Security and Management Conference, Edith Cowan University, Western Australia

Hoffman, C. (2014a, March 17). Your Home Router May Also Be a Public Hotspot — Don't Panic! Retrieved 23 August 2016, from http://www.howtogeek.com/184727/your-home-router-may- also-be-a-public-hotspot-dont-panic/

Hoffman, C. (2014b, April 21). Should You Buy a Router If Your ISP Gives You a Combined Router/Modem? Retrieved 23 August 2016, from http://www.howtogeek.com/187439/should - you-buy-a-router-if-your-isp-gives-you-a-combined-routermodem/

Horowitz, M. (2016, December 4). Firmware Updates - Router Security. Retrieved 15 October 2016, from http://routersecurity.org/firmware.updates.php

Independent Security Evaluators. (2015, April 22). SoHo_techreport.pdf. Retrieved 12 August 2016, from https://securityevaluators.com/knowledge/case_studies/routers/SoHo_techreport.pdf

Independent Security Evaluators, & Holcomb, J. (2013). Vulnerability_Catalog.pdf. Retrieved 2 October 2016, from https://securityevaluators.com/knowledge/case_studies/routers/Vulnerability_Catalog.pdf

Kidman, A. (2014, May 20). Telstra's New Wi-Fi Network: Everything You Need To Know. Retrieved 23 August 2016, from http://www.lifehacker.com.au/2014/05/telstras-new-wi-fi- network-everything-you-need-to-know/

Kim, P. (2017). Pwning the Dlink 850L routers and abusing the MyDlink Cloud protocol. Retrieved from https://pierrekim.github.io/blog/2017-09-08-dlink-850l-mydlink-cloud-0days-vulnerabilities.html

Laughlin, A. (n.d.). What is DLNA? - Which? Retrieved 2 October 2016, from http://www.which.co.uk/reviews/televisions/article/what-is-dlna

Land, J. (2017). Systematic Vulnerabilities in Customer-Premises Equipment (CPE) Routers. Retrieved from https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_502618.pdf

Netgear. (2011). ReadySHARE_Cloud_Flyer_12JULY2011.pdf. Retrieved 23 October 2016, from https://www.netgear.com/assets/landing/readyshare/ReadySHARE_Cloud_Flyer_12JULY2011.pdf

NIST. (2014). CVE-2013-3069: Multiple cross-site scripting (XSS) vulnerabilities in NETGEAR WNDR4700 with firmware 1.0.0.34 allow remote authenticate. Retrieved 23 October 2016, from http://www.cvedetails.com/cve/CVE-2013-3069/

Old-Computers.com. (n.d). OLD-COMPUTERS.COM Museum ~ Honeywell DDP-516. Retrieved 26 October 2016, from http://www.old-computers.com/museum/computer.asp?c=551&st=1

Out-Law.com. (2016, December 5). New law in Germany will further reduce liability of Wi-Fi providers for copyright infringement by users. Retrieved 16 October 2016, from http://www.out-law.com/en/articles/2016/may/new-law-in-germany-will-further-reduce- liability-of-wi-fi-providers-for-copyright-infringement-by-users/

Osborne, C. (2017). Researcher discloses 10 D-Link zero-day router flaws. Retrieved from http://www.zdnet.com/article/10-d-link-zero-day-router-flaws-exposed/

Raytheon. (2011, November 2). The ARPANET. Retrieved 8 October 2016, from http://www.raytheon.com/rtnwcm/groups/gallery/documents/digitalasset/rtn_224614.pdf

Rotenberg, N., Shulman, H., Waidner, M., Zeltser, B. (2017). *Authentication-Bypass Vulnerabilities in SOHO Routers*. Paper presented at ACM SIGCOMM 2017. UCLA Meyer & Renee Luskin Conference Center, LA

Router. (2016, August 23). UPnP. Retrieved from http://www.routercheck.com/upnp-2/

Router Check. (2016, August 23). CSRF. Retrieved from http://www.routercheck.com/csrf/

Sericon Technology. (2015, August 25). The_Real_State_of_WiFi_Security_in_the_Connected_Home.pdf. Retrieved 1 October 2016, from http://www.routercheck.com/WhitePapers/The_Real_State_of_WiFi_Security_in_the_Connected_Home.pdf

Shodan.io. (2016). Shodan. Retrieved 8 October 2016, from https://www.shodan.io/

Szewczyk, P. (2006). *Individuals' Perceptions of Wireless Security in the Home Environment*. Paper presented at the 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia

Szewczyk, P. (2013). *Usability and Security Support Offered Through ADSL Router User Manuals*. Paper presented at the 11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia

Szewczyk, P., & Valli, C. (2009). Insecurity by Obscurity: A Review of SoHo Router Literature from a Network Security Perspective. The Journal of Digital Forensics, Security and Law: JDFSL, 4(3), 5.

Telstra Corporation Limited (AU). (n.d.). Telstra Air - How it works - Telstra Wifi Network. Retrieved 23 August 2016, from https://www.telstra.com.au/broadband/telstra-air/how-it- works

Telstra Corporation Limited (AU). (2016a). Telstra - Wi-Fi Gateways & Extenders - Connected Home. Retrieved 15 October 2016, from https://www.telstra.com.au/connectedhome/enhancements/getwifi

Telstra Corporation Limited (AU). (2016b). Telstra Wifi Hotspot Network - Telstra Air. Retrieved 15 October 2016, from https://www.telstra.com.au/latest-offers/telstra-air-free-wifi-offer

US-CERT. (2011). HomeRouterSecurity2011.pdf. Retrieved 21 August 2016, from https://www.us-cert.gov/sites/default/files/publications/HomeRouterSecurity2011.pdf

Watkins, C. G. (2013). Wireless Liability: Liability Concerns for Operators of Unsecured Wireless Networks. Rutgers Law Review, Forthcoming, 2013.

Yang, L. (2016, April 15). [DS15] Advanced SoHo Router Exploitation - Lyon Yang. Retrieved 24 September 2016, from https://www.youtube.com/watch?v=vhR9gcTtx0g

